

## INSTRUCTIONS FOR THE PREPARATION OF FORM AD-1143

### Block No.

- 1 Check one or both
- 2 Enter the agency FFIS application number, i.e., FF34 for APHIS, or FF11 for Forest Service.
- 3 User's social security number (optional at this time).
- 4 User's name.
- 5 User's job title or contractor (if not an USDA employee).
- 6 Address where the user can be contacted by mail.
- 7 User's e-mail address.
- 8 User's phone number.
- 9 User's normal place of duty.
- 10 User's office symbols or organizational name.
- 11 User must sign and date, acknowledging user has read attached security rules before accessing or using FFIS or the Financial Data Warehouse.
- 12 Date signed
- 13 To be used when changing a user's name. Enter the user's "old" name.
- 14 To be used when changing a user's name. Enter the user's "new" name.
- 15 Check the appropriate action to be taken. If requesting to modify your profile, specify in block 17 the previous profile or job assignment and the new profile or job assignment.
- 16 Leave blank. The Agency Security Administrator will assign all FFIS and Financial Data Warehouse User ID's.
- 17 Specify the security profile or job assignment, or any comments or special instructions. For example, if the user's job role involves vendor payment disbursements, specify "Accounts Payable Clerk/Technician/Manager, as appropriate.
- 18 The user's manager must check whether a background investigation was initiated or completed.
- 19 Enter the month and year the background investigation was initiated or completed.
- 20 Print the name of the user's immediate manager.
- 21 Telephone number of the user's manager
- 22 Block must be signed and dated by user's immediate manager, indicating that he/she has approved the requested action.
- 23 FFIS Agency Security Administrator's signature.
- 24 Date Security Administrator completed user's request.

The Agency FFIS security administrator will retain each completed form for audit purposes.

**FOUNDATION FINANCIAL INFORMATION SYSTEM  
(FFIS) AND FINANCIAL DATA WAREHOUSE USER  
REGISTRATION/CHANGE REQUEST**

1. System Name (Check one or both)

☐ FFIS Application

☐ Financial Data Warehouse

2. FFIS Application Number \_\_\_\_\_

**User Information (See Privacy Statement on Reverse)**

3. User's SSN

4. User's name (last, first, middle initial)

5. User's title

6. User's mailing address

7. User's E-mail address

8. User's phone number

9. Post of Duty (Location)

10. Office

**User Acknowledgment**

I have read the automated information systems security rules on the reverse side of this form and understand the security requirements of the automated information systems and/ or applications described on this form. I understand disciplinary action, removal from the agency/USDA, and/or criminal prosecution may be taken based on violation of these rules.

11. User's signature

12. Date

**Action Requested**

**Name Change**

13. Old Name

14. New Name

**Access**

15. Check One

☐ Add User (Check all that apply.)

☐ Request for new password

☐ Delete User. Enter effective date: \_\_\_\_\_

☐ Modify user profile

16. FFIS User ID

17. Special instructions

**Background Investigation**

18. Check One

☐ Initiated

☐ Completed

19. Date (Initiated or  
Completed)

20. Print Manager's Name

21. Manager's Phone Number

**Authorization**

User's Manager - I certify the user has received security instructions for the systems and/or applications indicated, and I approve his/her access to these systems and/or applications, and the associated profiles.

22. Manager's Signature

**Action Taken**

23. Security Administrator Signature

24. Date

# FOUNDATION FINANCIAL INFORMATION SYSTEM (FFIS) SECURITY RULES

## **VIOLATION OF THESE RULES MAY RESULT IN DISCIPLINARY ACTION**

1. **DO NOT ACCESS**, research, or change any account, file, record or application not required to perform your official duties. You are forbidden to access your own account, that of a spouse, relative, friend, neighbor, or any account in which you have a personal or financial interest. If you are assigned to work on one of these accounts contact your supervisor.
2. If you are asked by another person to access an account or other sensitive or private information, **VERIFY** that the requested access is authorized. You will be held responsible if the access is not authorized. As a general rule, you should not use a computer or terminal in behalf of another person.
3. **PROTECT YOUR PASSWORD** from disclosure. You are responsible for any computer activity associated with your password. **DO NOT SHARE** your password with others or reveal it to anyone, regardless of his/her position in or outside the USDA. **DO NOT POST** your password in your work area. **DO NOT USE** another person's password. USER IDs must be treated with the same care as your password. Everything done with your user ID or password will be recorded as being done by you.
4. **PASSWORD DISTRIBUTION AND REFRESHMENT** must be done securely.
5. **CHANGE YOUR PASSWORD** if you think someone else knows your password. Immediately notify your supervisor, or the agency Functional Administrator or Security Administrator. Passwords for FFIS and the FFIS Data Warehouse will be changed every 30 days as prompted by the system.
6. **DO NOT PROGRAM** your login or password into automatic script routines or programs.
7. **LOG OFF/SIGN OFF** if you go to lunch, or break, or anytime you leave your computer or terminal.
8. **RETRIEVE ALL** hard copy printouts in a timely manner. If you cannot determine the originator or receiver of a printout, dispose of it in a burn waste container or shredder.
9. **IDENTIFY ALL** sensitive applications or data that you will be placing on a system, and any equipment processing sensitive information to your supervisor, so that appropriate security measures can be implemented.
10. **DO NOT USE USDA COMPUTERS** or software for personal use.
11. **DO NOT USE PERSONAL EQUIPMENT** or software for official business without your supervisor's written approval.
12. **DO NOT INSTALL OR USE UNAUTHORIZED SOFTWARE** on USDA equipment. Do not use freeware, shareware or public domain software on USDA computers, without your supervisor's permission and without scanning it for viruses. Comply with local office policy on the use of antiviral software.
13. **OBSERVE ALL SOFTWARE LICENSE AGREEMENTS.** Do not violate Federal copyright laws.
14. **DO NOT MOVE EQUIPMENT** or exchange system components without authorization by the appropriate functions and manager's approval.
15. **PROTECT USDA COMPUTER EQUIPMENT** from hazards such as liquids, food, smoke, staples, paper clips, etc.
16. **PROTECT MAGNETIC MEDIA** from exposure to electrical currents, extreme temperatures, bending, fluids, smoke, etc. Ensure the magnetic media is secured based on the sensitivity of the information contained, and practice proper labeling procedures. **BACK UP** critical programs and data, and store in a safe place. Back ups should be performed as often as program and data sensitivity require.
17. **DO NOT DISCLOSE THE TELEPHONE NUMBER(S)** or procedure(s) which permit system access from a remote location.
18. **DO NOT USE** sensitive information for equipment or program test purposes. Vendors should be escorted and monitored while performing maintenance duties.
19. **DO NOT DISCLOSE** or discuss any USDA personnel or vendor related information with unauthorized individuals. The Privacy Act of 1974, 5 USC 552a, prohibits such disclosure. A person making a willful unauthorized disclosure of information covered by this act may be charged with a misdemeanor and subject to a fine of up to \$5,000.
20. **PROMPTLY REPORT** all security incidents to your supervisor. For example: unauthorized disclosure of information, computer viruses, theft of equipment, software or information, and deliberate alteration or destruction of data or equipment.
21. Complete this form when Duties Change, when you separate from your agency, and to report name changes or request profile changes.

### Privacy Act Notice

In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of your Social Security Number is authorized by Executive Order 9397 of November 22, 1943 and 5 U.S.C. 301. The primary purpose of requesting the Social Security Number (SSN) is to properly identify the employee. Many employees have similar names and the furnishing of the SSN will enable USDA to identify authorized users of USDA's computer systems. The information will be used by offices and employees who have a need for the information in the performance of their official duties. The information will not be disclosed outside USDA. Disclosure of your SSN and other information is mandatory. Failure to provide the requested information will result in the denial of the requested computer access authority.